ProRail

Aan de Staatssecretaris van Infrastructuur en Milieu
Mevrouw W.J. Mansveld
Postbus 20901
2500 EX Den Haag

Datum	10 april 2015	Eigenaar	
Ons kenmerk	3732182	E-mail	
Onderwerp	Bijlage over ICT storingen op 22 januari en 2 februari		

Directie

Bezoekadres
HGB I
Moreelsepark 1
3512 EP Utrecht

Postadres
Postbus 2038
3500 GA Utrecht

Geachte mevrouw ,

In deze brief zullen wij conform uw vraag ingaan op de oorzaken van de storingen op 22 januari en 2 februari jl. Hierin wordt toegelicht wat de rol van ICT is op het spoor, wat er gebeurd is op 22 januari en 2 februari, wat de oorzaak was, en welke maatregelen zijn en worden genomen.

Er blijkt geen verband tussen beide storingen buiten uiteraard de fatale impact op het functioneren van de post Utrecht met grote reizigershinder tot gevolg. Het onderzoek naar de storing van 22 januari leidt tot een eenduidige conclusie ten aanzien van de oorzaak. De benodigde maatregelen zijn inmiddels uitgevoerd. Ten aanzien van de storing op 2 februari luidt een mogelijke conclusie dat een onbekende externe oorzaak dan wel een hardware probleem heeft geleid tot meerdere defecten en uiteindelijk tot de storing. Nader onderzoek hierop loopt nog omdat vooralsnog geen directe aanleiding kan worden gevonden. Hoe dan ook zijn meerdere maatregelen getroffen om de kans op herhaling te minimaliseren.

De rol van ICT op het spoor

ICT ligt aan de basis van vele ProRail en NS systemen. Voor het ProRail deel van de treinbesturing volgen hier enkele cijfers: er zijn 3 landelijke computercentra (Nieuwegein, Amsterdam en Utrecht), 13 regionale computercentra in verkeersleidingsposten, 1 testcentrum, 1 uitwijkcentrum. In totaal betreft het meer dan 300 centrale computers voor de besturing van treinen en meer dan 500 locaties met technische IT. De 13 regionale verkeersleidingsposten zijn nodig voor het besturen van het treinverkeer. Elke post heeft voor de directe treinbesturing vier verschillende en onderling samenwerkende type ICT systemen nodig. Dit zijn:

1. Computer (postcluster-hardware omgeving): Dit behelst het centrale computersysteem op elke regionale post die bestaat uit meerdere computers (vijf of zeven, afhankelijk van de omvang en het bediengebied van de post) en twee opslagsystemen. Het geheel is redundant uitgevoerd.
2. Software (applicatielaag): op het postcluster draait de software die de treindienstleiders nodig hebben voor de besturing van de treinen (omleggen van wissels, besturing van seinen, volgen van treinen, etc).

3. Netwerk: netwerk verbindt het postcluster met de onderposten langs de spoorbaan welke het laatste deel van de computers richting de infrastructuur zijn. Van de ICT richting de infrastructuur dus.
4. Telefonie (GSM-R): GSM-R biedt de treindienstleider de mogelijkheid om machinisten te spreken dan wel een noodoproep te doen naar meerdere treinen in een gebied. Telefoniecentrales van de posten staan in verbinding met de landelijke GSM-R centrale die weer de verbinding heeft naar de zendmasten langs het spoor.

Op de 13 regionale posten zijn al deze vier systemen vertegenwoordigd. Als een van de 52 systemen (4 systemen x 13 gebieden) in het land niet functioneert, rijden in dat gebied geen treinen. Elk van deze vier systemen per verkeersleidingspost is cruciaal voor het functioneren, en dus is elk van deze vier systemen per verkeersleidingspost redundant uitgevoerd. Door het organiseren van deze redundantie in de afgelopen zeven jaar, heeft ProRail het aantal ICT storingen en de impact ervan met meer dan 80% gereduceerd. Nog steeds kan het echter voorkomen dat een van de vier deelsystemen stoort en daarmee uitval van een post geeft op een van de dertien posten. In de afgelopen jaren hebben we gemiddeld één tot twee storingen per jaar gehad (in dus één van de 52 deelsystemen) die voor de post fataal waren.

De treindienstleider op de post bestuurt de treinen in een bepaald gebied. Naast de treindienstleider is er ook een verkeersleider. Deze overziet een groter gebied. Hij komt vooral in actie bij grote verstoringen. Hij maakt hierbij gebruik van een landelijk verkeersleidingssysteem. Het verkeersleidingssysteem geeft aanpassingen door naar de verschillende posten en dus naar het systeem van de treindienstleider. Daarnaast geeft het ook de aanpassingen door naar het landelijke reisinformatiesysteem (voor de borden en automatische omroep en digitale reisinformatie zoals op de site of app). Het verkeersleidingssysteem komt dus eigenlijk pas in actie als bijsturing noodzakelijk is en niet meer mogelijk is op het niveau van de post.

Na de brand van de verkeersleidingspost Utrecht in 2010 is besloten het postcluster met daarop de applicaties voor de treinbesturing in een van de landelijke computercentra te plaatsen.

Wat is er feitelijk gebeurd met de systemen van de verkeersleidingspost Utrecht op 22 januari en 2 februari?

Donderdag 22 januari

Op 22 januari vond een storing plaats in het netwerk tussen de regionale verkeersleidingspost Utrecht en het landelijke computercentrum in Nieuwegein. In het netwerk ontstond een ongecontroleerde hoeveelheid aan dataverkeer. Daardoor raakte het netwerk verstopt en werd de communicatie tussen de werkplek van de treindienstleider en het computercentrum gedurende 18 minuten ernstig verstoord. Dientengevolge duurde de feitelijke uitval van de werkplekken op de verkeersleidingspost Utrecht ongeveer 40 minuten. Dat komt omdat na uitval de computerprogramma's tijd nodig hebben om hun verbindingen te herstellen en het beeld van de feitelijke situatie buiten weer op te bouwen.

Wat was de oorzaak van 22 januari?

Uitgebreid onderzoek naar de storing op 22 januari geeft met zekerheid aan dat het een netwerkstoring betrof en dat de aanleiding van de storing een eerdere aanpassing in het netwerk is geweest. Aanpassingen (variërend van aard en impact) vinden voortdurend plaats. Afhankelijk van het risico van zo'n aanpassing wordt die overdag of 's nachts gepland. De aanpassing op 22 januari was beoordeeld als laag risico en overdag ingepland. Helaas bleek dat het netwerk zich anders gedroeg omdat een instelling in een aanpalend het netwerk van NS zich slecht verhield tot de instellingen in het netwerk van ProRail. De netwerken van NS en ProRail zijn logischerwijs verbonden, omdat het proces van verkeersleiding en het proces van besturing van materieel & personeel een ketenproces is. De aangetroffen verkeerde instellingen zijn direct gecorrigeerd. Aanvullende beschermende maatregelen zijn aangebracht opdat wederzijdse beïnvloeding van netwerken niet meer kan plaatsvinden. Alle netwerken zijn vanzelfsprekend op vergelijkbare zaken gecontroleerd en ook daar zijn zo nodig risico's weggenomen. Het onderzoek naar deze storing is afgerond en een vergelijkbaar risico is inmiddels uitgesloten.

Maandag 2 februari

De storing op maandagochtend 2 februari begon met het uitvallen van een computer uit het postcluster van Utrecht in het landelijke computercentrum in Nieuwegein rond 7.30 uur. Dergelijke computers zijn redundant uitgevoerd en dus nam een andere computer onmiddellijk over. Even na het overschakelen naar de redundante computer ontstond er echter een tweede defect in het systeem. In een van de twee dataopslagsystemen (die elkaar kunnen opvangen) ging een controllerkaart kapot. In elk van de twee dataopslagsystemen zitten twee van deze controllerkaarten die ook elkaar moeten opvangen. Bij het opvangen van dit defect in het opslagsysteem werd het systeem echter instabiel en traag. Het gehele systeem functioneerde veel trager dan noodzakelijk voor het bedienen van de seinen en wissels door de treindienstleiders. Het niet langer kunnen bedienen van de seinen en de wissels leidde tot de grote verstoring rondom Utrecht. Uiteindelijk viel het opslagsysteem als geheel uit waardoor het andere opslagsysteem het uiteindelijk goed kon overnemen. Daarmee kwam de redundantie weer terug en kwam het verkeersleidingsysteem weer op snelheid.

Wat was de oorzaak van 2 februari?

De belangrijkste conclusie uit de verschillende externe onderzoeken is dat er geen eenduidige, initiële oorzaak of fout van de twee hardware defecten op 2 februari is gevonden. Omdat de defecten, waarvan de tweede heeft geleid tot de storing, in korte tijd achter elkaar optraden, was eerst de breed gedeelde aanname -ook van externe onderzoekers- dat er één externe oorzaak zou moeten zijn geweest. Deze is echter vooralsnog niet aangetroffen. Het onderzoek loopt nog steeds, hetgeen echter bemoeilijkt wordt doordat veel onderdelen inmiddels preventief zijn vervangen of gewijzigd. De reden dat de redundantie zo traag op gang is gekomen, is wel duidelijk: de oorzaak hiervoor lag in een overbelasting van het opslagsysteem doordat kort na het uitvallen van één computer ook nog eens de controllerkaart in het opslagsysteem kapot ging. De combinatie werd na analyse door zowel software partner Intraffic als leverancier HP als funest beschouwd. Het systeem kon alle dataverwerking die ontstond door de inwerking tredende processen voor redundantie van eerst de computer en bijna direct erna de controllerkaart niet meer aan. Er ontstonden time outs en de besturingssystemen reageerden daarop met aanvullende acties. De trage werking is door de

leverancier van de hardware als uitzonderlijk bestempeld - veroorzaakt door een zeldzame combinatie van defecten. Toen het opslagsysteem uiteindelijk volledig uitviel en overschakelde naar een tweede opslagsysteem, functioneerde het systeem weer zoals het hoort. ProRail heeft nu in afstemming met de leverancier een passend afhandelscenario gedefinieerd voor het geval dit uitzonderlijke systeemgedrag nogmaals zou optreden.

Maatregelen ter voorkoming

ProRail heeft diverse maatregelen genomen om incidenten als deze in de toekomst te voorkomen. Ten aanzien van de netwerkstoring op 22 januari zijn technische maatregelen in de instellingen van het ICT netwerk genomen, zoals het instellen van een blokkade op een mogelijke beïnvloeding van het ProRail-netwerk door instellingen in een ander (gekoppeld) netwerk. Deze maatregelen zijn in aanvulling op security maatregelen die ProRail jaarlijks ook extern laat beoordelen. ProRail en NS hebben verder verbeterde afspraken gemaakt over het uitwisselen van informatie in het geval van aanpassingen (changes) en toekomstige ontwikkelingen van elkaars netwerk.

Ten aanzien van de trage redundantie op 2 februari leidt onderzoek tot de conclusie dat de kans op tegelijk een defecte computer en een defect in het opslagsysteem zeer klein wordt geacht. Als dit zich dan toch voordoet en het opslag systeem zich op eenzelfde manier traag zou herstellen dan kan met een directe handeling op het opslagsysteem, ervoor gezorgd worden dat alsnog de redundantie van het andere opslagsysteem snel in werking treedt.

Op verschillende terreinen heeft ProRail aanvullend externe expertise ingeschakeld:

- De status van het netwerk, het ontstaan van de storing en mogelijke restrisico's en daarbij voorstellen tot maatregelen (Thales)
- Het gedrag van de verschillende software applicaties op het systeem van Utrecht bij het optreden van de hardware defecten (Intraffic in samenwerking met CGI)
- Welke defecten zijn ontstaan in de hardware en de mogelijke achtergrond van het ontstaan van die defecten en de wijze waarop de redundantie in de hardware heeft gefunctioneerd in combinatie met de software (HP)
- De wijze waarop onderzoek is uitgevoerd en de geformuleerde maatregelen passend zijn (PBLQ)
- Aanvullend minutieus onderzoek op de defecten in hardware en aanwijzingen op het mogelijk ontstaan ervan (TNO)
- Inzet van tegendenker in team om tunnelvisie te voorkomen (Corion)
- Onderzoek naar opzet voedingsconcept en of hierin aanwijzingen kunnen worden gevonden voor het ontstaan van de hardware defecten (DNVGL)

Uit de hierboven genoemde onderzoeken komt geen aanbeveling of noodzaak tot breder of nader onderzoek. Ook een verificatie van het ICT systeem als geheel wordt door de experts niet nodig geacht, aangezien de conclusie is dat het ICT systeem degelijk en goed functioneert. ProRail heeft - vanwege de grote afhankelijkheid van ICT-systemen in de operatie - desondanks zelf besloten nog een extra extern onderzoek te laten doen door TNO. Dit onderzoek richt zich op de status van de hardware en het mogelijk achterhalen van de oorzaak van de eerder gevonden defecten in componenten van de hardware opdat alle onzekerheid hieromtrent kan worden uitgesloten.

Resultaten van dit onderzoek waren nog niet beschikbaar bij het versturen van deze brief. Wij verwachten dat de resultaten van dit onderzoek eind april beschikbaar komen.

Conclusie

Vanwege de grote afhankelijkheid van ICT-systemen in de operatie heeft ProRail de analyse van de incidenten met grote prioriteit en aandacht opgepakt. Sinds 2 februari heeft een ICT taskforce zich intensief bezig gehouden met de interne en externe onderzoeken, zijn de conclusies en tussenrapportages uitvoerig intern besproken en zijn maatregelen getroffen. De conclusies van de verschillende onderzoeken geven aan dat de kans op herhaling van een storing met dezelfde oorzaak in de systemen klein is, zeker met de genomen maatregelen. We blijven echter scherp op risico's, ook deze storing heeft ons doen beseffen dat ondanks alle maatregelen die eerder zijn genomen een storing met deze impact nog steeds niet kan worden uitgesloten. De directie blijft daarom zeer alert op de kwaliteit en risico's van ICT, en blijft ICT regulier agenderen. Het aantreden van een Commissaris met als aandachtsgebied ICT markeert het belang dat ICT heeft voor het spoor: onze Raad van Commissarissen wordt regulier en intensief betrokken bij de verdere ontwikkeling van ICT.

Met vriendelijke groet,

P. Eringa
President-directeur